Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims:

Claims 1 to 30 (canceled)

31. (currently amended) A method of establishing a session key between a pair of correspondents in a data communication system, each of said correspondents sharing secret information [[(d)]], said method comprising the steps of:

a) one of said correspondents generating additional secret information [[(k)]] and deriving therefrom a session key;

b) said one of said correspondents ~~transferring said additional~~ combining said secret information [[(k)]] ~~to the other of said correspondents;~~ and said additional secret information in a signature algorithm to provide a first signature component;

c) said one of said correspondents deriving a second signature component from said secret information;

d) said one of said correspondents transferring said first and second signature components to the other of said correspondents;

[[c)]] e) said other of said correspondents using said secret information [[(d)]] ~~and said~~ to obtain said additional secret information [[(k)]] from said first signature component and generating ~~to generate a~~ said session key [[.]] from said secret information and said additional secret information; and

f) said other of said correspondents verifying said second signature component by operating upon said session key obtained at said other of said correspondents to obtain a value corresponding to said second signature component and comparing such value with said second signature component.

32. (cancelled)

33. (currently amended) A method of claim [[32]] 31 wherein said first signature component includes public information associated with said other correspondent and said other

correspondent utilizes said public information to obtain said additional secret information.

34. (currently amended) A method according to claim 33 wherein said secret information [[(d)]] and [[said]] public information [[(Q_B)]] are combined in said signature algorithm and such combination is precomputed and stored by said one correspondent.

35. (previously presented) A method according to claim 34 wherein said combination is the product of said secret information and said public information.

36. (cancelled)

37. (currently amended) A method according to claim [[36]] 31 wherein a portion of said ~~shared key~~ secret information is utilized to provide said second signature component.

38. (currently amended) A method according to claim 37 wherein said ~~shared key~~ secret information represents the coordinates of a point on an elliptic curve and said portion is one of said coordinates.

39. (previously presented) A method according to claim 37 wherein said portion is hashed by a secure hash function to provide said second signature component.

40. (cancelled)

41. (currently amended) A method of establishing a session key between a first correspondent and a selected one of a plurality of second ~~corespondents corrected~~ correspondents connected to said first correspondent, said method comprising providing each of said second correspondents a respective secret information[[,]]; storing each [[of]] said secret ~~informations~~ information at said first correspondent to associate each [[of]] said stored secret ~~informations~~ information with a respective second correspondent[[,]]; said selected one of said second correspondents combing said secret information and additional secret information in a signature algorithm to provide a first signature component, said additional secret information being used

by said selected correspondent to generate a session key; said selected one of said second correspondents deriving a second signature component from said secret information; said first correspondent receiving from said selected one of said second correspondents [[a]] said first and second signature components; ~~including a first component combining said secret information with additional secret information used by said selected one of said second correspondents to generate a session key,~~ said first correspondent retrieving said stored secret information associated with said selected one of said second correspondents and using said secret information to obtain [[and]] said additional secret information ~~to generate a~~ and generating said session key from said secret information of said selected one of said second correspondents and said additional secret information; and ~~corresponding to the session key of said selected one of said second correspondents.~~ said first correspondent verifying said second signature component by operating upon said session key obtained at said first correspondent to obtain a value corresponding to said second signature component and comparing such value with said second signature component.

42. (cancelled)

43. (currently amended) A method of claim [[42]] 41 wherein said first signature component includes public information associated with said first correspondent and said first correspondent utilizes said public information to obtain said additional secret information.

44. (cancelled)

45. (currently amended) A method according to claim [[44]] 41 wherein a portion of said ~~shared key~~ secret information is utilized to provide said second signature component.

46. (currently amended) A method according to claim 45 wherein said ~~shared key~~ secret information represents the coordinates of a point on an elliptic curve and said portion is one of said coordinates.

47. (previously presented) A method according to claim 45 wherein said portion is hashed by

a secure hash function to provide said second signature component.

48. (cancelled)